УДК 512.552

С. В. Гольдберг

СЛОЖНОСТЬ ПРОВЕРКИ ТОЖДЕСТВ В ПОЛУГРУППАХ ПРЕОБРАЗОВАНИЙ РАНГА 2*

Введение

Под задачей проверки тождеств понимается следующая комбинаторная задача распознавания, имеющая в качестве параметра заданную конечную алгебру $\mathcal{A}$:

УСЛОВИЕ: задано тождество $p = q$.

ВОПРОС: Выполнено ли тождество $p = q$ в алгебре $\mathcal{A}$?

Задачу проверки тождеств для данной алгебры $\mathcal{A}$ будем обозначать через CHECK-ID($\mathcal{A}$).

В последнее время заметное внимание привлекает проблема классификации конечных алгебр по вычислительной сложности** проверки тождеств в них. Оказывается, что для некоторых алгебр (например, для диэдральных групп, см. [3]) можно подтвердить или опровергнуть справедливость любого тождества за время, ограниченное полиномом от его длины, а для некоторых других (например, для неразрешимых групп, см. [4]) при стандартном предположении $\mathsf{P} \neq \mathsf{NP}$ полиномиального алгоритма проверки тождеств не существует.

Пока по сложности проверки тождеств удалось полностью классифицировать ассоциативные кольца [5], существенные продвижения имеются для групп, а вот ситуация в классе полугрупп представляется весьма запутанной. Исследования в этой области ведутся различными группами математиков (см. [6–12]).

Естественно попытаться классифицировать по сложности проверки тождеств некоторые наиболее важные полугруппы, такие, как полугруппы преобразований. На настоящий момент для полугруппы всех преобразований n-элементного множества получен следующий «почти полный» результат.

---

*Работа выполнена при поддержке программы «Развитие научного потенциала высшей школы», проект № 2.1.1/3537.

**Сложность алгоритмов в настоящей работе понимается в смысле монографий [1, 2], там же читатель сможет найти определения упоминаемых в работе классов сложности P и co-NP.

Теорема 1. [7] *Задача проверки тождеств в полугруппе всех преобразований n-элементного множества* co-NP*-полна при $n = 3$ и $n \geqslant 5$ и решается за полиномиальное время при $n = 1, 2$.*

Здесь мы рассмотрим полугруппы $T_2(n)$, состоящие из всех преобразований n-элементного множества с не более чем 2-элементным образом. Полученные на сегодняшний день результаты работ [13, 14] фактически утверждают полиномиальную разрешимость задачи CHECK-ID() для полугруппы $T_2(n)$ при всех $n \neq 3$. Результат же данной работы показывает, что случай $n = 3$ резко отличается от всех остальных.

Теорема 2. *Задача проверки тождеств в полугруппе $T_2(n)$ всех преобразований ранга не более 2 над n-элементным множеством является полиномиально разрешимой при $n \neq 3$ и* co-NP*-полной при $n = 3$.*

1. Определения и обозначения

Обозначим полугруппу всех преобразований на множестве X через $T(X)$, а в случае $|X| = n$ полугруппу всех преобразований n-элементного множества обозначим через $T(n)$. Через $T_k(X)$ (соответственно $T_k(n)$) будем обозначать множество всех таких преобразований из $T(X)$ (соответственно $T(n)$), образ которых состоит из не более k элементов.

Мы будем записывать преобразования справа от аргумента; произведение двух преобразований в $T(n)$ – это результат их последовательного выполнения в том порядке, в котором они записаны. Отметим, что на сложность задачи проверки тождеств это соглашение не влияет, – полугруппа $\overleftarrow{T}(n)$ всех преобразований n-элементного множества, действующих справа налево, антиизоморфна $T(n)$ и удовлетворяет некоторому тождеству тогда и только тогда, когда в $T(n)$ выполняется зеркальное отражение этого тождества.

Все утверждения, в том числе из работ других авторов, мы будем формулировать в терминах преобразований, действующих слева направо.

Пусть Σ – некоторый алфавит. Обозначим множество букв, входящих в слово $w \in \Sigma^+$, через $\chi(w)$, а через $\chi^2(w)$ – множество 2-факторов, входящих в слово w.

Кратностью буквы $x \in \Sigma$ в слове $w \in \Sigma^+$ назовем число различных вхождений x в w в качестве фактора, т. е. число различных представлений вида $w = uxv$, где u, v – возможно пустые слова. Кратность буквы x в слове w будем обозначать через $\ell_x(w)$.

Аналогично, определим *кратность 2-фактора* $xy \in \chi^2(w)$ и обозначим ее через $\ell_{xy}(w)$.

Через $\mathrm{suff}_x(w)$ обозначим максимальный суффикс слова w, не содержащий вхождения буквы x. Заметим, что $\mathrm{suff}_x(w) = w$, если x не входит в w. Через $\mathrm{suff}_{xy}(w)$ обозначим максимальный суффикс слова w, не содержащий вхождения 2-фактора xy.

Так как в данной работе нас будут интересовать факторполугруппы Риса вида $T_n(m)/T_1(m)$ по идеалу $T_1(m)$, то напомним определение. Пусть I – идеал полугруппы S. Определим отношение ρ на S, полагая $a\rho b$ $(a, b \in S)$ тогда и только тогда, когда либо $a = b$, либо a и b принадлежат I. Отношение ρ называется *конгруэнцией Риса по модулю* I. Классами эквивалентности полугруппы S по модулю ρ являются само I и каждое одноэлементное множество $\{a\}$, где $a \in S \setminus I$. Вместо S/ρ пишется S/I и S/I называется *факторполугруппой Риса полугруппы* S *по модулю* I. Можно представлять себе S/I как результат сжатия I в один элемент (нуль), в то время как элементы из $S \setminus I$ не затрагиваются.

2. Легкость проверки тождеств в $T_2(n)$ при $n \neq 3$

В этом параграфе мы обсудим, почему же задача проверки тождеств в полугруппах $T_2(n)$ при $n \neq 3$ решается за полиномиальное от длины входного тождества время. Приведя здесь формулировки критериев выполнения тождеств, мы продемонстрируем их схожесть во всех полугруппах преобразований $T_2(n)$, кроме случая $n = 3$.

2.1. CHECK-ID($T(2)$)

Сложность задачи CHECK-ID($T(2)$) подробно обсуждалась в работе [7]. Мы приведем здесь основные тезисы.

Прежде всего, отметим, что полугруппа $T(2)$ четырехэлементна, что позволяет применить результат Климы [10, предложение 4], согласно которому задача CHECK-ID($\mathcal{S}$) разрешима за полиномиальное время для любой не более чем пятиэлементной полугруппы $\mathcal{S}$ с единицей.

Однако, если не опираться ни на общий результат Климы, ни на используемые им в доказательстве результаты диссертации Тессона [15], то можно доказать следующий критерий выполнения тождества в полугруппе $T(2)$.

Предложение 1 [7, предложение 2.1]. *Тождество $p = q$ справедливо в полугруппе $T(2)$ тогда и только тогда, когда для любой буквы x (не обязательно встречающейся в словах p и q)*

(1) $\chi(\mathrm{suff}_x(p)) = \chi(\mathrm{suff}_x(q))$;

(2) $\forall\, y \ \ \ell_y(\mathrm{suff}_x(p)) = \ell_y(\mathrm{suff}_x(q)) \mod 2$.

Ясно, что условия предложения 1 можно проверить за полиномиальное (в действительности даже за линейное) время от суммы длин слов p и q.

2.2. CHECK-ID($T_2(X)$). *Результат Н. Г. Торлоповой*

Тождества полугруппы $\overleftarrow{T_2}(X)$ были исследованы в работе [13]. Естественно, что в 1982 г. ни о какой вычислительной сложности задачи проверки тождеств речи не велось. Поэтому мы сначала приведем здесь доказанный Торлоповой критерий выполнения тождеств в полугруппе $T_2(X)$, а затем опишем примерный алгоритм проверки данного критерия и оценим его временную сложность.

В соответствии с принятым нами соглашением все условия выполнения тождества в полугруппе $\overleftarrow{T_2}(X)$ переформулируем так, чтобы получились условия выполнения тождества в полугруппе $T_2(X)$.

Будем говорить, что тождество $p = q$ удовлетворяет условию (2factor), если

a. $\chi^2(p) = \chi^2(q)$;

b. $\forall\, xy \in \chi^2(p) \;\; \ell_{xy}(p) = \ell_{xy}(q) \mod 2$.

Предложение 2. *Пусть X-счетное множество. В полугруппе $T_2(X)$ всех преобразований ранга не более 2 множества X тождество $p = q$ выполняется тогда и только тогда, когда*

(1) первые буквы слов p и q совпадают;

(2) тождество $p = q$ и все суффиксные подтождества вида $\mathrm{suff}_{xy}(p) = \mathrm{suff}_{xy}(q)$ удовлетворяют условию (2factor).

Интересно отметить, что из критерия выполнения тождества в данной полугруппе вытекает, что любое суффиксное подтождество по 2-фактору выполненного в полугруппе тождества также выполнено в полугруппе.

Важным следствием из хода доказательства приведенного предложения является следующее

Следствие 2.1. *Многообразие, порожденное полугруппой $T_2(X)$, совпадает с многообразием, порожденным полугруппой $T_2(n)$, для всех $n \geqslant 5$.*

Алгоритм задачи CHECK-ID($T_2(X)$)

Мы приведем алгоритм решения задачи проверки тождеств в полугруппе $T_2(X)$ и оценим его временную сложность. Основная часть алгоритма связана с проверкой условия (2factor) для самого тождества и всех его суффиксных подтождеств.

Для проверки условия (2factor) для тождества $p = q$:

Шаг 1. Проходим по словам p и q для формирования списка 2-факторов; для каждого 2-фактора сохраняем количества его вхождений в слово p и q. Время этой операции можно с запасом оценить как $|p|^2 + |q|^2$.

Шаг 2. Осуществляем линейный проход по списку 2-факторов (время порядка $|p| + |q|$) и проверяем следующие условия:

$$\ell_{xy}(p) = \ell_{xy}(q) \mod 2 \ \text{ и } \ \ell_{xy}(p) \cdot \ell_{xy}(q) \neq 0.$$

Так как мы прямо в списке храним величины $\ell_{xy}()$, алгоритмически эта операция ничего не стоит.

Дальнейшая часть алгоритма будет выполняться лишь в том случае, если $\chi^2(p) = \chi^2(q)$, поэтому длину списка 2-факторов можно оценивать как $|p|$.

Для построения всевозможных суффиксных тождеств вида $\operatorname{suff}_{xy}(p) = \operatorname{suff}_{xy}(q)$ нам достаточно пройтись по списку 2-факторов и для каждого xy из этого списка выделить первое с конца слова его вхождение в p и q. Эта операция может ничего не стоить по времени, если сразу при построении списка 2-факторов запомнить индекс последнего вхождения фактора в слово p и q.

Далее для каждого суффиксного тождества вида $\operatorname{suff}_{xy}(p) = \operatorname{suff}_{xy}(q)$ (это цикл по $xy \in \chi^2(p)$) нам необходимо проверить выполнение условия (2factor).

Такую проверку можно сразу оценить по времени как

$$|\operatorname{suff}_{xy}(p)|^2 + |\operatorname{suff}_{xy}(q)|^2 + |p|,$$

сославшись на приведенный выше алгоритм для тождества $p = q$, если не задумываться о трате памяти на построение нового списка 2-факторов.

Если же попытаться обойтись уже существующим списком 2-факторов, то алгоритм можно реализовать следующий:

Шаг 3. Проходим по существующему списку 2-факторов, проходим по словам $\operatorname{suff}_{xy}(p)$ и $\operatorname{suff}_{xy}(q)$ и заменяем $\ell_{zt}(p)$ на $\ell_{zt}(\operatorname{suff}_{xy}(p))$, $\ell_{zt}(q)$ на $\ell_{zt}(\operatorname{suff}_{xy}(q))$. Время можно оценить как

$$|\operatorname{suff}_{xy}(p)| \cdot |p| + |\operatorname{suff}_{xy}(q)| \cdot |p| < |p|^2 + |q|^2.$$

Шаг 4. За линейное время порядка $|p|$ проверяем выполнение следующих условий:

$$\ell_{zt}(\operatorname{suff}_{xy}(p)) = 0 \ \Leftrightarrow \ \ell_{zt}(\operatorname{suff}_{xy}(q)) = 0,$$

$$\ell_{zt}(\operatorname{suff}_{xy}(p)) = \ell_{zt}(\operatorname{suff}_{xy}(q)) \mod 2.$$

В итоге проверка условия (2factor) для каждого суффиксного тождества занимает по времени порядка

$$|p| \cdot (|p|^2 + |q|^2 + |p|) < (|p| + |q|)^3.$$

Суммарная временная сложность алгоритма оценивается кубическим полиномом от длины тождества.

По памяти можно ограничиться одним списком 2-факторов, чья совокупная длина оценивается как $5(|p| + |q|)$, и массивами для хранения слов p, q и всех их суффиксов по 2-факторам.

Таким образом, мы получили полиномиальную разрешимость задачи CHECK-ID($T_2(n)$) для всех $n \geqslant 5$.

2.3. CHECK-ID($T_2(4)$). *Результат Г. И. Машевицкого*

В работе [14] утверждается, что задача проверки тождеств в полугруппе $\overleftarrow{T_2}(4)$ полиномиально разрешима. Мы приведем здесь критерий выполнимости тождеств, переформулировав его для полугруппы $T_2(4)$.

Прежде всего, в работе Машевицкого отмечается тот факт, что задача проверки тождеств полиномиально разрешима в факторполугруппе Риса $T_2(4)/T_1(4)$.

Предложение 3. *Тождество $p = q$ выполнено в полугруппе $T_2(4)/T_1(4)$ тогда и только тогда, когда*

(1) *первые буквы слов p и q совпадают, последние буквы слов p и q совпадают;*

(2) $\chi^2(p) = \chi^2(q)$;

(3) $\forall\, xy \in \chi^2(p) \;\; \ell_{xy}(p) = \ell_{xy}(q) \mod 2$.

Критерий выполнимости тождества в самой полугруппе $T_2(4)$ выглядит следующим образом.

Предложение 4. *Тождество $p = q$ выполнено в полугруппе $T_2(4)$ тогда и только тогда, когда*

(1) *первые буквы слов p и q совпадают, последние буквы слов p и q совпадают;*

(2) $\chi^2(p) = \chi^2(q)$;

(3) $\forall\, xy \in \chi^2(p) \;\; \ell_{xy}(p) = \ell_{xy}(q) \mod 2$;

(4) *все суффиксные тождества вида* $\mathrm{suff}_x(p) = \mathrm{suff}_x(q)$ *удовлетворяют условиям* (1)–(3);

(5) *все суффиксные тождества вида* $\mathrm{suff}_{xy}(p) = \mathrm{suff}_{xy}(q)$ *удовлетворяют следующим условиям:*

(a) *первые буквы слов тождества совпадают, последние буквы слов тождества совпадают;*

(b) $\chi^2(\mathrm{suff}_{xy}(p)) = \chi^2(\mathrm{suff}_{xy}(q))$;

(c) $(\forall\, k)\ \ \ell_k(\mathrm{suff}_{xy}(p)) = \ell_k(\mathrm{suff}_{xy}(p)) \mod 2$;

(d) $(\forall\, k)\ \ \ell_{xk}(\mathrm{suff}_{xy}(p)) = \ell_k(\mathrm{suff}_{xy}(p)) \mod 2$ *и*
$\ell_{ky}(\mathrm{suff}_{xy}(p)) = \ell_{ky}(\mathrm{suff}_{xy}(p)) \mod 2$;

(e) $(\forall\, k, m)$ *из того, что* $ky \notin \chi^2(\mathrm{suff}_{xy}(p))$, *следует, что* $\ell_{km}(\mathrm{suff}_{xy}(p)) = \ell_{km}(\mathrm{suff}_{xy}(p)) \mod 2$;

(f) $(\forall\, k, m)$ *из того, что* $xk \notin \chi^2(\mathrm{suff}_{xy}(p))$, *следует, что* $\ell_{mk}(\mathrm{suff}_{xy}(p)) = \ell_{mk}(\mathrm{suff}_{xy}(p)) \mod 2$.

Несложно понять, соотнеся данный критерий с результатом Торлоповой, что проверка условий предложения 4 требует полиномиального от длины входного тождества времени.

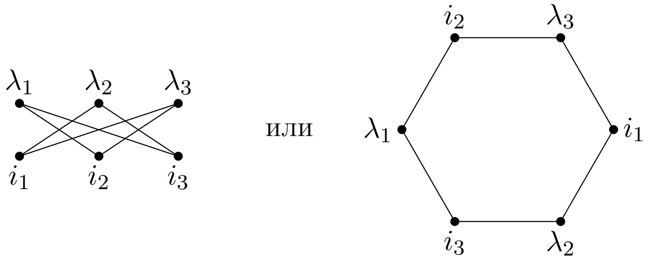
3. Сложность проверки тождеств в $T_2(3)$

Этот параграф посвящен доказательству «сложности» проверки тождеств в полугруппе $T_2(3)$. Доказательство будет основано на полиномиальном сведении задачи CHECK-ID($T_2(3)/T_1(3)$) к задаче CHECK-ID($T_2(3)$). Вычислительная сложность задачи проверки тождеств в полугруппе $T_2(3)/T_1(3)$, а именно ее co-NP-полнота, была установлена в работе [6] (интересно сравнить этот результат с предложением 3).

Для того чтобы сформулировать критерий выполнимости тождества в полугруппе $T_2(3)/T_1(3)$, приведем необходимые определения из работы [6].

3.1. Необходимые определения

Под *двудольным графом* понимается тройка (V, W, E), где V и W – непересекающиеся множества вершин графа (две доли графа), а E – множество ребер вида (ϑ, ω), где $\vartheta \in V$ и $\omega \in W$. Под *мультиграфами* понимаются графы с кратными ребрами: множество ребер E рассматривается как мультимножество, а кратностью ребра (ϑ, ω) соответственно называется мощность множества $\{e \in E : e = (\vartheta, \omega)\}$.



Графы шестиугольника

Важную роль в работе [6] играл (двудольный) граф шестиугольника (см. рисунок); будем в дальнейшем обозначать его через Hex.

Для произвольного слова p определим двудольный граф $G_p(V_p, W_p, E_p)$. Для этого по каждой букве x_k слова p зададим две вершины $a_k \in V_p$ и $b_k \in W_p$; ребра построим по правилу: $(a_k, b_l) \in E_p$ тогда и только тогда, когда слово p содержит 2-фактор $x_k x_l$.

Дополнительно для каждого слова p мы определим двудольный мультиграф $\widetilde{G_p}(V_p, W_p, \widetilde{E_p})$. Для этого каждому ребру (a_k, b_ℓ) обыкновенного графа $G_p(V_p, W_p, E_p)$ припишем кратность, равную числу появления фактора $x_k x_\ell$ в слове p.

Пусть $G_p = G_q$. Множества ребер $\widetilde{E_p}$ и $\widetilde{E_q}$ соответствующих мультиграфов $\widetilde{G_p}$ и $\widetilde{G_q}$ можно объединить как мультимножества: $\widetilde{E_p} \biguplus \widetilde{E_q}$ состоит из множества всех ребер $E_p = E_q$ в качестве носителя, и каждое ребро получает кратность, равную сумме его кратностей в мультиграфах $\widetilde{G_p}$ и $\widetilde{G_q}$. Тем самым мы получим мультиграф $\widetilde{UG} = (V_p, W_p, \widetilde{E_p} \biguplus \widetilde{E_q})$, который в дальнейшем будем называть *объединением мультиграфов* $\widetilde{G_p}$ и $\widetilde{G_q}$ и обозначать через $\widetilde{UG} = \widetilde{G_p} \uplus \widetilde{G_q}$.

Под гомоморфизмом $\varphi : G \to G'$ мультиграфа $G = (V, W, E)$ на обыкновенный граф $G' = (V', W', E')$ мы будем понимать отображение множеств вершин $\varphi : V \cup W \to V' \cup W'$, сохраняющее отношение «быть ребром» (из условия $(\vartheta, \omega) \in E$ следует, что $(\varphi(\vartheta), \varphi(\omega)) \in E'$). Образом ребра (ϑ, ω) при гомоморфизме φ в таком случае будем называть ребро $(\varphi(\vartheta), \varphi(\omega))$.

Под *двудольным гомоморфизмом* $\varphi : G \to G'$ двудольного мультиграфа $G = (V, W, E)$ на обыкновенный двудольный граф $G' = (V', W', E')$ мы будем понимать гомоморфизм, сохраняющий отношение «принадлежать разным долям» (из условий $\vartheta \in V$ и $\omega \in W$ следует, что $\varphi(\vartheta)$ и $\varphi(\omega)$ принадлежат разным долям графа G').

Теперь мы готовы сформулировать критерий выполнимости тождеств в полугруппе $T_2(3)/T_1(3)$.

Предложение 5. *Тождество $p = q$ выполнено в полугруппе $T_2(3)/T_1(3)$ тогда и только тогда, когда*

(1) $G_p = G_q$ *(это эквивалентно тому, что $\chi^2(p) = \chi^2(q)$);*

(2) *первые буквы слов p и q совпадают, последние буквы слов p и q совпадают;*

(3) *для каждой буквы x четность числа ее вхождений в левую и правую части тождества одинакова, т. е. $\ell_x(p) = \ell_x(q) \mod 2$;*

(4′) *для произвольного двудольного гомоморфизма $\varphi : \widetilde{UG} \to Hex$ каждое ребро $(\lambda, i) \in Hex$ имеет четный по мощности прообраз, т. е.*

$$|\varphi^{-1}(\lambda, i)| = 0 \mod 2.$$

Лемма 1 [6, лемма 7.1]. *Пусть даны двудольные мультиграфы $\widetilde{G}$ и $\widetilde{G_1}$ такие, что соответствующие им обыкновенные графы G и G_1 совпадают. Если для каждого ребра графа $G = G_1$ четность его кратности совпадает в $\widetilde{G}$ и $\widetilde{G_1}$, то графы $\widetilde{G}$ и $\widetilde{G}_1$ удовлетворяют условию* **4′** *одновременно.*

Лемма 1 перестает быть верной, если убрать требование совпадения обыкновенных графов: в общем случае не верно, что ребра нулевой кратности можно заменить на ребра с четной кратностью с сохранением условия **4′**. Тем не менее верна следующая лемма.

Лемма 2 [6, лемма 7.2]. *Пусть дан двудольный граф $\widetilde{G}$, имеющий изолированные вершины. Пусть граф $\widetilde{G}_1$ получен из исходного добавлением новых четных по кратности ребер, соединяющих изолированные вершины с неизолированными так, что каждая изолированная вершина смежна максимум с одной неизолированной. Тогда графы $\widetilde{G}$ и $\widetilde{G}_1$ удовлетворяют условию* **4′** *одновременно.*

3.2. Доказательство co-NP*-полноты* CHECK-ID($T_2(3)$)

Если тождество $p = q$ выполнено в полугруппе $T_2(3)$, то оно выполнено в полугруппе $T_2(3)/T_1(3)$. Или, что эквивалентно, если тождество $p = q$ не выполнено в полугруппе $T_2(3)/T_1(3)$, то оно не выполнено в полугруппе $T_2(3)$.

Понятно, что нарушение импликации ($p \neq q$ в $T_2(3) \Rightarrow p \neq q$ в $T_2(3)/T_1(3)$) может быть только в том случае, если существует такая подстановка из $T_2(3)$, что p и q означиваются разными элементами из идеала $T_1(3)$.

Лемма 3. *Пусть дано тождество $p = q$ такое, что*

(1) $G_p = G_q$;

(2) *p является суффиксом слова q.*

Тогда при означивании тождества в полугруппе $T_2(3)$ слова p и q попадают в идеал $T_1(3)$ одновременно, причем принимают одинаковые значения.

Доказательство. В работе [6] (см. замечание 6.1) подробно обсуждалось, что условие совпадения графов слов отвечает за одновременное обращение слов в 0 при произвольном означивании тождества в полугруппе $T_2(3)/T_1(3)$. Следовательно, в полугруппе $T_2(3)$ совпадение графов слов отвечает за одновременное попадание означенных слов в идеал $T_1(3)$.

Обозначим через $i \in T_1(3)$ результат означивания слова p. Так как слово p является суффиксом слова q, а ранг преобразования i равен 1, то значением вычисленного слова q будет также элемент i.

Если мы ограничимся рассмотрением только таких тождеств, которые фигурируют в лемме 3, то импликация ($p \neq q$ в $T_2(3) \Rightarrow p \neq q$ в $T_2(3)/T_1(3)$) становится верной. Значит, при таком ограничении задача проверки тождеств в полугруппе $T_2(3)$ эквивалентна задаче проверки тождеств в полугруппе $T_2(3)/T_1(3)$. Осталось доказать следующую теорему.

Предложение 6. *Задача проверки тождеств $p = q$ таких, что*

(1) $G_p = G_q$;

(2) *первые буквы слов p и q совпадают, последние буквы слов p и q совпадают;*

(3) *для каждой буквы четность числа ее вхождений в левую и правую части тождества одинакова;*

(4) *p является суффиксом слова q;*

в $T_2(3)/T_1(3)$ остается co-NP*-полной.*

Доказательство. Первые три условия являются необходимыми условиями выполнения тождества в полугруппе $T_2(3)/T_1(3)$, причем полиномиально проверяемыми. Следовательно, нам остается доказать, что ограничение (4) на тождества не уменьшает сложность задачи CHECK-ID($T_2(3)/T_1(3)$). Для этого полиномиально сведем задачу проверки тождеств, удовлетворяющих условиям (1)–(3), к задаче проверки тождеств, удовлетворяющих условиям (1)–(4).

По заданному тождеству $p = q$ построим новое тождество $p' = q'$, удовлетворяющее условию (4) теоремы, такое что

$$(p = q \quad \text{в} \quad T_2(3)/T_1(3) \quad \Leftrightarrow \quad p' = q' \quad \text{в} \quad T_2(3)/T_1(3)).$$

Пусть $p = xuy,\ q = xvy$.

Рассмотрим двудольный мультиграф $\widetilde{G_p}$. Добавим к этому графу новую пару вершин c и d и припишем этой паре новую букву z.

Положим

$$p' = zxuyz,$$
$$q' = zxvy(zxuy)^2 z.$$

Очевидно, что $G_{p'} = G_{q'}$ и что первые и последние буквы слов p' и q' совпадают. Более того, слова p' и q' удовлетворяют условию (3) критерия выполнимости тождества в полугруппе $T_2(3)/T_1(3)$, так как $\ell_z(p') = 2$, $\ell_z(q') = 4$ и кратности всех остальных букв в слове p' не изменились по сравнению со словом p, а в слове q', по сравнению со словом q, увеличились лишь на четное число (в связи с добавлением удвоенного слова p).

Кроме того, в графе $\widetilde{UG'} = \widetilde{G_{p'}} \uplus \widetilde{G_{q'}}$ по сравнению с исходным графом $\widetilde{UG}$ кратности всех старых ребер увеличились на четное число – на удвоенное количество ребер графа $\widetilde{G_p}$, а кратности новых ребер из вершин c и d равны 4. Следовательно, $\widetilde{UG'} = \widetilde{UG} \mod 2$. Таким образом, по совокупности лемм 1 и 2 графы $\widetilde{UG'}$ и $\widetilde{UG}$ удовлетворяют условию $\mathbf{4'}$ одновременно.

Значит, задачи выполнения тождеств $p = q$ и $p' = q'$ в полугруппе $T_2(3)/T_1(3)$ эквивалентны.

Осталось отметить тот несложный факт, что из co-NP-полноты ограничения задачи проверки тождеств на множество входных тождеств вида $p = wp$ немедленно следует co-NP-полнота задачи проверки любых тождеств.

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

2. Papadimitriou C. H. Computational complexity. Reading, Mass.: Addison-Wesley, 1994.

3. Burris S., Lawrence J. Results on the equivalence problem for finite groups // Algebra Universalis. 2005. Vol. 52. P. 495–500.

4. Horváth G., Lawrence J., Mérai L. et al. The complexity of the equivalence problem for nonsolvable groups // Bull. London Math. Soc. 2007. Vol. 39. P. 433–438.

5. Burris S., Lawrence J. The equivalence problem for finite rings // J. Symbolic Comput. 1993. Vol. 15. P. 67–71.

6. Плещева С. В., Вертеши В. Сложность задачи проверки тождеств в 0-простой полугруппе // Изв. Урал. гос. ун-та. 2006. № 43. (Компьютерные науки и информационные технологии; Вып. 1). С. 72–102.

7. Алмейда Ж., Волков М. В., Гольдберг С. В. Сложность задачи проверки тождеств в конечных полугруппах // Зап. науч. семинаров ПОМИ. 2008. Т. 358. (Исследования по конструктивной математике и математической логике; Вып. XI). С. 5–22.

8. Jackson M., McKenzie R. Interpreting graph colorability in finite semigroups // Internat. J. Algebra Comput. 2006. Vol. 16, № 1. P. 119–140.

9. Kisielewicz A. Complexity of semigroup identity checking // Ibid. 2004. Vol. 14, № 4. P. 455–464.

10. Klíma O. Complexity issues of checking identities in finite monoids // Semigroup Forum. 2009. Vol. 79, № 3.

11. Seif S. The Perkins semigroup has co-NP-complete term-equivalence problem // Internat. J. Algebra Comput. 2005. Vol. 15, № 2. P. 317–326.

12. Seif S., Szabó Cs. Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields // Semigroup Forum. 2006. Vol. 72, № 2. P. 207–222.

13. Торлопова Н. Г. О полугруппах ранга 2 / Ленингр. гос. пед ин-т. Л., 1982. 22 с. Деп. в ВИНИТИ 15.11.82, № 5590-82.

14. Mashevitzky G. Bases of identities of semigroups of a bounded rank transformations of a set, manuscript, 2007.

15. Tesson P. Computational complexity questions related to finite monoids and semigroups: Ph.D. Thesis / McGill University. Montréal, 2003.

Статья поступила 08.14.2008